Blackberry Forensics

SANS DFIR Summit 2014 – Austin TX

Shafik G. Punja
Cindy Murphy

June-9-14

TEELtechnologies

SPEAKER BACKGROUND

- **Shafik G. Punja**
    - Active duty LE, performing digital forensics since Nov 2003
    - Instructor for Teel Technologies US and Canada
    - Senior Technical Officer – QuByte Logic Ltd
    - Private sector work involves R n D partnerships with various LE colleagues, digital forensics training, data analytics and consulting services.
    - Shameless plug: Course developer and primary instructor for Advanced BlackBerry Forensics Class: http://www.teeltech.com/tt3/blackberry4.asp?cid=16

SPEAKER BACKGROUND

- **Cindy Murphy**
  - Detective, City of Madison, WI Police Department since 1991, LE Officer since 1985
  - Involved in DFIR since 1998
  - MSc Forensic Computing and Cyber Crime Investigation from University College, Dublin – 2011
  - Shameless plug: SANS 585 Advanced Smartphone Forensics – Coauthor & Instructor
  - http://www.sans.org/event/for585-advanced-smartphone-mobile-device-forensics

1.0. UNLOCKED BLACKBERRY DEVICES

Unlocked BlackBerry device with no password

Situation

- BB contains memory card and SIM.
- Which type of data extraction should be performed and in what order?
- Physical, File System, then Logical?

Examiner Considerations:

- There are a variety of tools available to the examiner.
- Start Physical, if supported,then move to File System and Logical.
  - Wear Leveling
  - A data structure at the logical level, in the form of a logical backup/acquisition is different than the same record at the physical level.
- ** In **rare cases** performing a physical with UFED may cause device to reset itself to factory default.
  - This referred by Cellebrite as “cache memory reset”.

BlackBerry ID

You need to sign in with your BlackBerry ID to use BBM, BlackBerry World and more.

Learn more about BlackBerry ID

If you already have a BlackBerry ID, **sign in** now. If you're new to BlackBerry, you need to **create** a BlackBerry ID.

Not sure if you already have a BlackBerry ID?
Learn how to check if you have a BlackBerry ID

Create New
Sign in

Swipe left to skip

1.0. UNLOCKED BLACKBERRY DEVICES

Unlocked BlackBerry device with password

Situation

- Password not known and cannot be removed
- Fortunately, the device desktop is accessible and can be navigated.
- To prevent a time out due to inactivity the device must be 'used’ (i.e. keep the mouse moving).

Examiner Considerations:

- Password not known and cannot be removed.
- Device data can be viewed, and your only recourse is to take pictures.

2.0. LOCKED BLACKBERRY DEVICES

Locked BlackBerry - Not attached to BES:

Situation:

- Shows only one padlock in lower right.
- Contains no memory card.

Examiner Considerations:

- Password NOT stored on computer or laptop that device is synced with.
- Password is NOT found within the IPD or BBB backup file.
- There is no 'lockdown' type file.
- In the absence of the password, only recourse is chipoff extraction.

June-9-14

TEELtechnologies

2.0. LOCKED BLACKBERRY DEVICES

Locked BlackBerry - Attached to BES:

Situation:

- Internal investigation, device is managed by a BES.
- Showing two padlocks: upper left and lower right.
- BES is accessible to the examiner.

Examiner Considerations:

- Initiate a password reset to device through BES
  - PW reset will not destroy user data
- Physical image obtained with UFED
  - Tool may not decrypt the encrypted content if BES encryption policies are in place.
  - May also be influenced by the BlackBerry OS version.
- UFED PA Decryption capability depends on the BB OS involved.
  - Newer encryption methods are not supported.
- Turning off/disabling the encryption to the device will only affect new data.
- In any BES related scenarios don’t forget to check the BES logs & Email Server!
  - Call history, Messaging and emails

2.0. LOCKED BLACKBERRY DEVICES

Locked BlackBerry attached to BES with PGP encryption:

Situation:

- External BES, managed by hostile entity
- Showing two padlocks: upper left and lower right
- Investigators found a sticky note with the password: 'secret'.
- Physical image (because of known password) was obtained through UFED tools.
- Email was PGP encrypted, and is encrypted within UFED PA.

Examiner Considerations:

- UFED PA Decryption capability depends on the BB OS involved.
    - Newer encryption methods are not supported.
- When pass code is entered on the BlackBerry, email is unlocked/decrypted
    - You have to unlock each email individually, by sender
- You will have to photograph each email item!
    - No known tool capable of decrypting PGP encrypted email content, even with password.
- There has been success with setting up a new bogus account & new IT policy
    - Have the BB talk with an active directory server.
    - Only after the BB sync completed, was the email downloaded in unencrypted state.

2.0. LOCKED BLACKBERRY DEVICES

Locked BlackBerry, not attached to BES

Situation

- Showing two padlocks: upper left and lower right
- Contains a memory card.

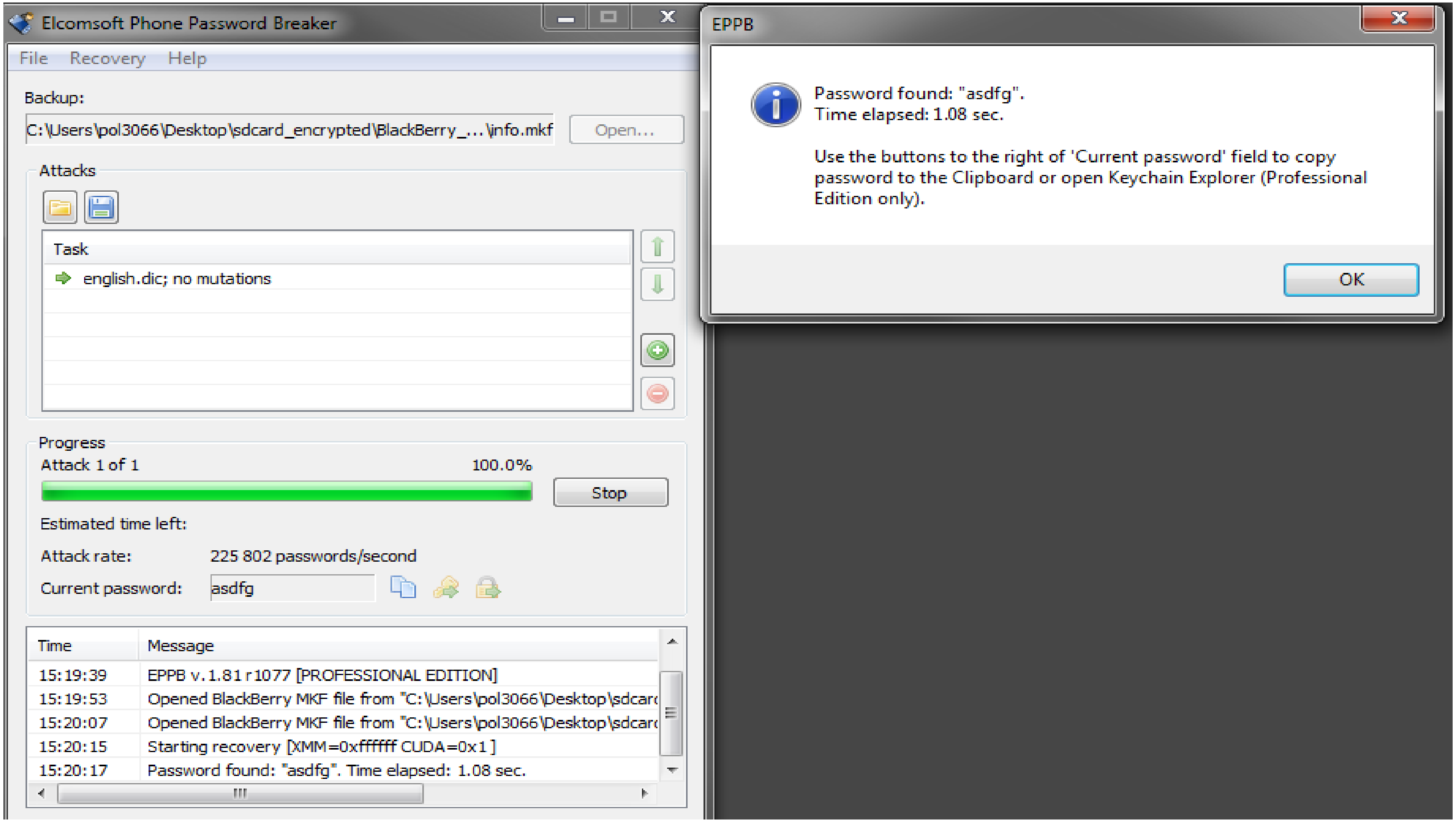
Examiner Considerations:

- Password NOT stored on computer or laptop that device is synced with.
- Password is NOT found within the IPD or BBB backup file.
- There is no 'lockdown' type file.
- Image memory card, and locate the **info.mkf file**
- Use Elcomsoft Phone Password Breaker (EPPB) to analyze and obtain password.
- In the absence of the password only recourse is chipoff extraction of memory.

June-9-14

TEELtechnologies

Locked BlackBerry – info.mkf file



Backup: C:\Users\pol3066\Desktop\sdcard_encrypted\BlackBerry_...\info.mkf

english.dic; no mutations

Attack 1 of 1 100.0%

Estimated time left:

Attack rate: 225 802 passwords/second

Current password: asdfg

```
Time      Message
15:19:39  EPPB v.1.81 r1077 [PROFESSIONAL EDITION]
15:19:53  Opened BlackBerry MKF file from "C:\Users\pol3066\Desktop\sdcard
15:20:07  Opened BlackBerry MKF file from "C:\Users\pol3066\Desktop\sdcard
15:20:15  Starting recovery [XMM=0xffffff CUDA=0x1]
15:20:17  Password found: "asdfg". Time elapsed: 1.08 sec.
```

Password found: "asdfg".
Time elapsed: 1.08 sec.

Use the buttons to the right of 'Current password' field to copy password to the Clipboard or open Keychain Explorer (Professional Edition only).

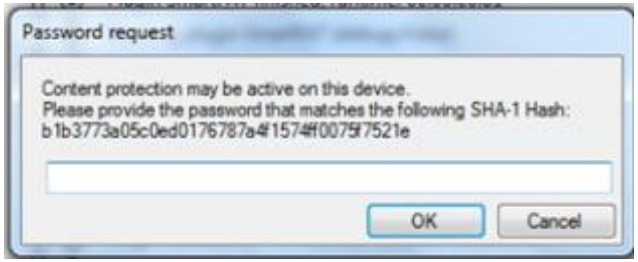
June-9-14

2.0. LOCKED BLACKBERRY DEVICES

Locked BlackBerry – Completed Successful Chipoff

Situation:

- Showing two padlocks: upper left and lower right.
- No success with memory card and attack of info.mkf file.
- Successful de-chipping and reading of the chip.
- During parsing by UFED PA message is provided to examiner:



Password request

Content protection may be active on this device.
Please provide the password that matches the following SHA-1 Hash:
b1b3773a05c0ed0176787a4f1574ff0075f7521e

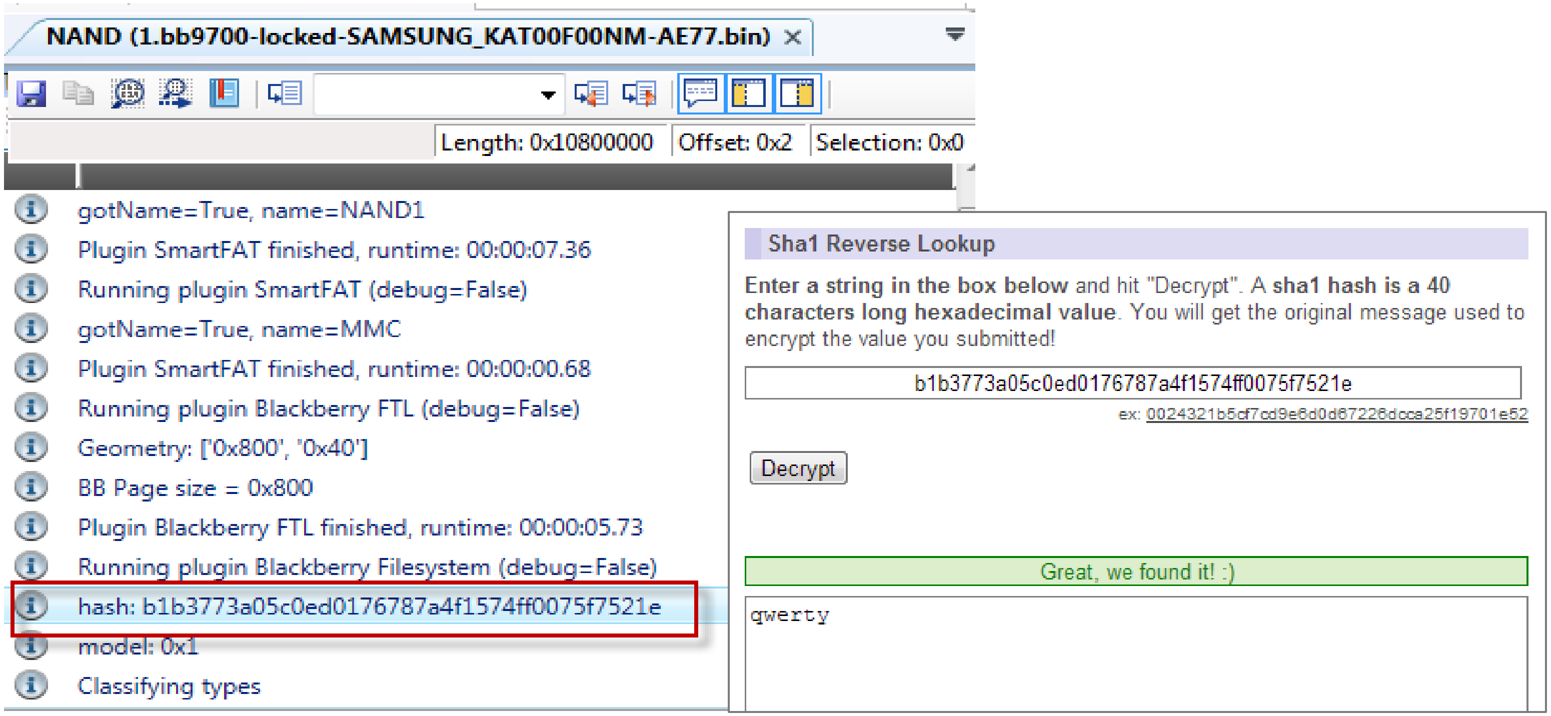
Examiner Considerations:

- Copy SHA1 value and use one of several, freely available online sources to decrypt the SHA1 value; enter the decoded SHA1 value into the UFED PA screen.

June-9-14

Locked BlackBerry – SHA1 Password

- The hash value is a 40 characters in length, which is typically indicative of SHA1 value.



Length: 0x10800000 Offset: 0x2 Selection: 0x0

```
gotName=True, name=NAND1
Plugin SmartFAT finished, runtime: 00:00:07.36
Running plugin SmartFAT (debug=False)
gotName=True, name=MMC
Plugin SmartFAT finished, runtime: 00:00:00.68
Running plugin Blackberry FTL (debug=False)
Geometry: ['0x800', '0x40']
BB Page size = 0x800
Plugin Blackberry FTL finished, runtime: 00:00:05.73
Running plugin Blackberry Filesystem (debug=False)
hash: b1b3773a05c0ed0176787a4f1574ff0075f7521e
model: 0x1
Classifying types
```

Sha1 Reverse Lookup

Enter a string in the box below and hit "Decrypt". A **sha1 hash is a 40 characters long hexadecimal value**. You will get the original message used to encrypt the value you submitted!

b1b3773a05c0ed0176787a4f1574ff0075f7521e

ex: 0024321b5cf7cd9e6d0d67226dcca25f19701e52

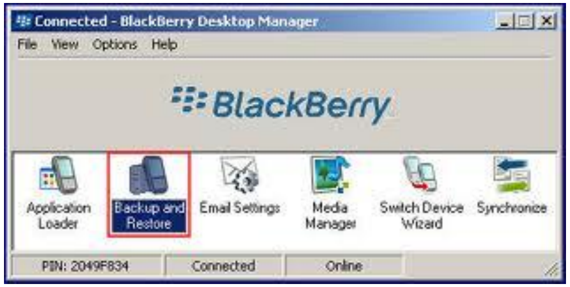
Great, we found it! :)

qwerty

June-9-14

TEELtechnologies

3.0. BLACKBERRY BACKUP FILES



BlackBerry Backup File IPD

Situation:

- Encrypted and unencrypted IPD files found during analysis of hard drive image.

Examiner Considerations:

- Parse unencrypted IPD files with an IPD tool that will detect the Phone History database structure
  - This is NOT the same as the Phone Call Log.
- Attempt decryption of encrypted IPD files using Elcomsoft Phone Password Breaker (EPPB).
- Decrypted files can be parsed with IPD decoding tools.

3.0. BLACKBERRY BACKUP FILES

Disconnected - BlackBerry Desktop Manager

BlackBerry Desktop Manager

- OPTIONS
- HELP

- Media Manager
  Manage songs, ringtones, videos, and pictures for your BlackBerry device.
- Synchronize
  Change options for synchronizing email messages and organizer data.
- Backup and Restore
  Back up or restore your BlackBerry device data.
- Application Loader
  Add, update, or remove BlackBerry device applications.
- Email Settings
  Create email message filters or change message forwarding options.
- Switch Device Wizard
  Transfer data from a BlackBerry device or other device to a BlackBerry device.

SERVER STATUS: Not logged in | DEVICE CONNECTED (PIN): None | Check For Updates

BlackBerry Backup File BBB

Situation:

- Encrypted and unencrypted BBB files found during analysis of hard drive image.

Examiner Considerations:

- BBB is the newer backup format used for BlackBerry Desktop Software 7.x (Windows).
- Parse unencrypted BBB files with an tool that understands the BBB backup structure.
  - BBB files contain a PK file header signature.
- Attempt decryption of encrypted BBB files using Elcomsoft Phone Password Breaker (EPPB).
  - Decrypted files can be parsed with BBB decoding tools.

4.0. BLACKBERRY MESSENGER (BBM)

BBM Chat CSV File

Situation:

- BBM chat files in CSV format found during analysis of memory card image.

Examiner Considerations:

- Date/Time is 21 digit numeric value: YYYYMMDD (first 8 digits) followed by remaining13 decimal values - unix DATE AND TIME stamp (numeric values in millisecond).
- There may CON and BAK files present, which contain the BBM user's contacts and a backup of the contacts.

4.0. BLACKBERRY MESSENGER (BBM)

BBM 5.0: No Chat history saved

Situation:

- BBM version 5.0 is being used on device, and saving of chat history is not enabled.

Examiner Considerations:

- Must do a physical extraction with UFED tool, in order to obtain BBM chat data.
- Enabling the save chat history feature only affects new chat from the date the option is enabled - will not work on chat conversations currently on the device.
- If physical extraction not possible, then only recourse is to take pictures.

4.0. BLACKBERRY MESSENGER (BBM)

BBM Database File: bbm.db

Situation:

- BBM version 6.0 is being used on device; examination of logical extraction shows a bbm.db file.

Examiner Considerations:

- Proprietary database that contains BBM chat **even if** option of saving chat history was **NOT** enabled.
- Most recent chat artifacts may not be present in the bbm.db file.
- Tools that address the parsing of this file:
  - UFED PA
  - Oxygen Forensic Suite (OFS).

4.0. BLACKBERRY MESSENGER (BBM)

BBM Conversations Folder

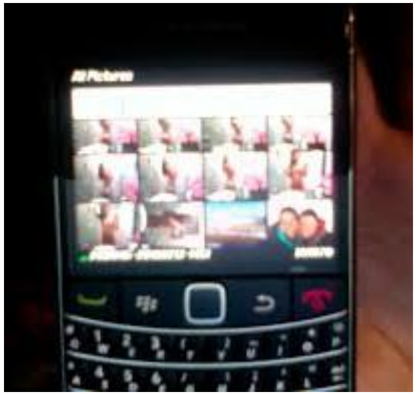
Situation:

- Examiner is reviewing a logical extraction, and observes within the data structure a folder called BBM Conversations.
- A manual examination of the file contained within this folder shows that it contains BBM chat.
- The BlackBerry is using BlackBerry OS 7.x.

Examiner Considerations:

- The file within the BBM Conversations Folders is similar in structure to the bbm.db file.
- There is one tool that does decode this structure:
    - BlackBerry Backup Explorer (Reincubate).

5.0. BLACKBERRY ARTIFACTS:



BBThumbs.dat, key/dat

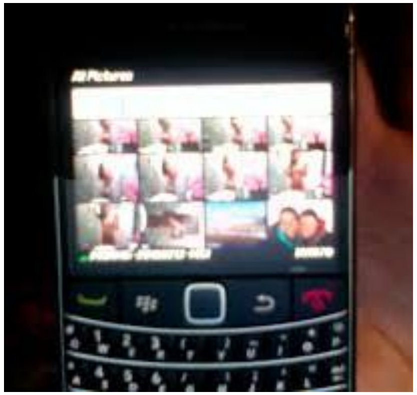
Situation:

- Examiner is reviewing a BB logical extraction, and MicroSD Card image associated to the BlackBerry device.
- There is need to locate and identify victim related child exploitation content present on the device and/or memory card.

Examiner Considerations:

- DAT or KEY/DAT files contain thumbnail cache of pictures currently or previously stored on the BlackBerry device or its associated memory card.
- If the DAT file is associated to video, then it only tracks the filename of the video file that used to exist.
- Several open source and commercial tools that can parse these files.

5.0. BLACKBERRY ARTIFACTS:



EXIF: BlackBerry device created movie and pictures

Situation:

- Examiner is reviewing a BB logical extraction, and the MicroSD Card image associated to the BlackBerry device.
- There is need to identify how the pictures and movie files, related to a child exploitation investigation were created.

Examiner Considerations:

- Pictures:
  - Can contain geotag data along with traditional date/time values, and make/model values.
- Movies:
  - No geo tagging or make/model embedded within movie files; usual time stamps values for media creation embedded within the video file; the encoder value called **"rimm"** will be observed.
- Best tool to use is ExifTool (Phil Harvey)

5.0. BLACKBERRY ARTIFACTS:

EXIF timestamp mismatch

Situation:

- EXIF original date/time embedded within a photo taken by the Blackberry 8310 had the incorrect time stamp.

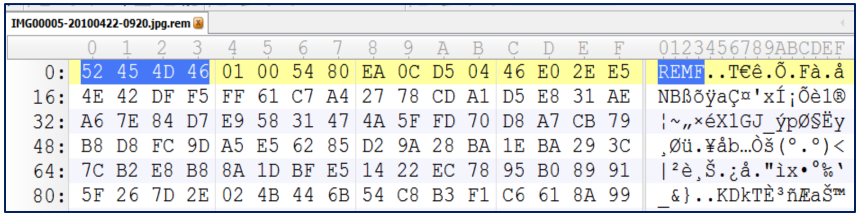
Examiner Considerations:

- Presumption:
  - BlackBerry is writing the correct time value to EXIF data when a photo is taken with a BlackBerry device.
- Issue:
  - When device goes to sleep or into screensaver mode, the device clock 'stops' or 'freezes'.
  - When the BlackBerry device is brought out of either mode, and a picture is taken, 'frozen' device time value will be written to the EXIF data of the first picture taken.
  - This typically does not affect subsequent pictures, as the device clock will update.

June-9-14

5.0. BLACKBERRY ARTIFACTS:

REMF Files



IMG00005-20100422-0920.jpg.rem

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
  0: 52 45 4D 46 01 00 54 80 EA 0C D5 04 46 E0 2E E5   REMF..T€ê.Õ.Fà.å
 16: 4E 42 DF F5 FF 61 C7 A4 27 78 CD A1 D5 E8 31 AE   NBßõÿaÇ¤'xÍ¡Õè1®
 32: A6 7E 84 D7 E9 58 31 47 4A 5F FD 70 D8 A7 CB 79   ¦~„×éX1GJ_ýpØ§Ëy
 48: B8 D8 FC 9D A5 E5 62 85 D2 9A 28 BA 1E BA 29 3C   ¸Øü.¥åb…Òš(°.°)<
 64: 7C B2 E8 B8 8A 1D BF E5 14 22 EC 78 95 B0 89 91   |²è¸Š.¿å."ìx•°‰'
 80: 5F 26 7D 2E 02 4B 44 6B 54 C8 B3 F1 C6 61 8A 99   _&}..KDkTÈ³ñÆaŠ™
```

Situation:

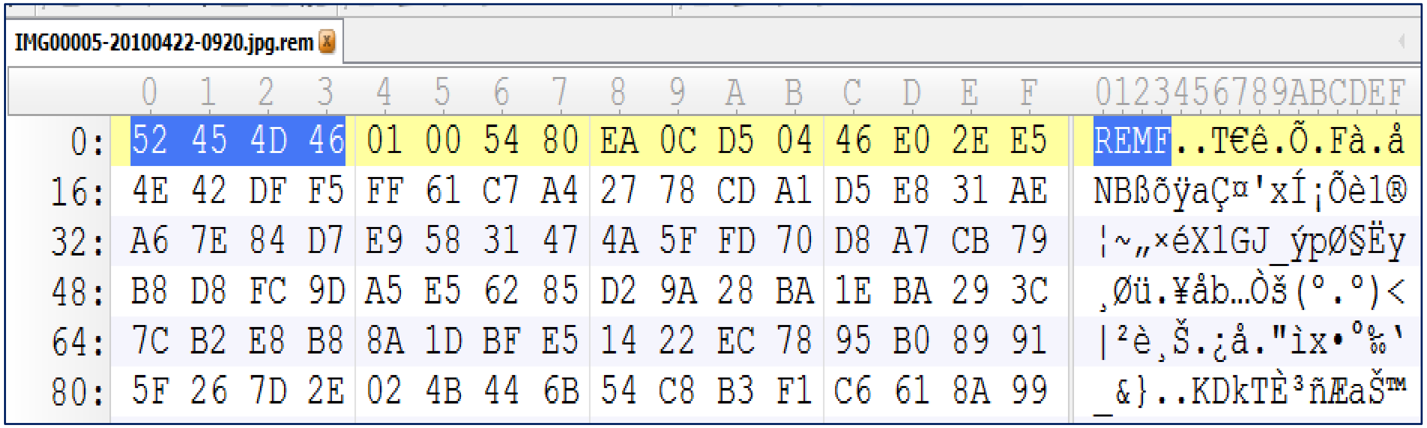
- Examiner discovers a number of files on the memory card and the BlackBerry device that end with the extension '.rem'.
- File header of these files is: '**REMF**'.

Examiner Considerations:

- REM extension at the end of a file denotes an encrypted file
  - Can only be decrypted by the device that encrypted the files.
- If the device is using BlackBerry OS 6 and lower
  - Placing the memory card in another device same make, model and OS, can decrypt the '.rem' files.
  - Alternately using a BlackBerry simulator that matches of the original device will also work.
  - This loophole was fixed in BlackBerry OS 7.
- Another method is to use the latest version of UFED PA, or Elcomsoft Phone Password Breaker and see if the .rem files can be decrypted.

BlackBerry – Artifacts REMF

- Looking at the file header of a rem encrypted JPG image we can see the header in ASCII is "REMF", or 52 45 4D 46h.

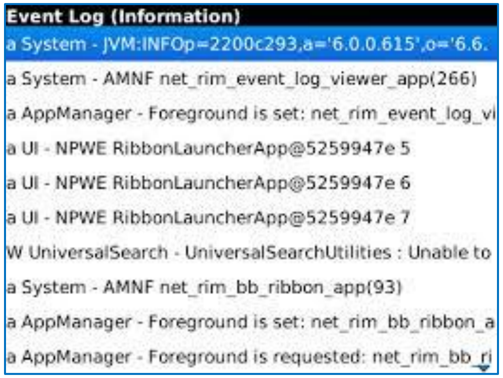


IMG00005-20100422-0920.jpg.rem

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
  0: 52 45 4D 46 01 00 54 80 EA 0C D5 04 46 E0 2E E5   REMF..T€ê.Õ.Fà.å
 16: 4E 42 DF F5 FF 61 C7 A4 27 78 CD A1 D5 E8 31 AE   NBßõÿaÇ¤'xÍ¡Õè1®
 32: A6 7E 84 D7 E9 58 31 47 4A 5F FD 70 D8 A7 CB 79   ¦~„×éX1GJ_ýpØ§Ëy
 48: B8 D8 FC 9D A5 E5 62 85 D2 9A 28 BA 1E BA 29 3C   ¸Øü.¥åb…Òš(º.º)<
 64: 7C B2 E8 B8 8A 1D BF E5 14 22 EC 78 95 B0 89 91   |²è¸Š.¿å."ìx•°‰'
 80: 5F 26 7D 2E 02 4B 44 6B 54 C8 B3 F1 C6 61 8A 99   _&}..KDkTÈ³ñÆaŠ™
```

June-9-14

6.0. BLACKBERRY EVENT LOGS



```
Event Log (Information)
a System - JVM:INFOp=2200c293,a='6.0.0.615',o='6.6.
a System - AMNF net_rim_event_log_viewer_app(266)
a AppManager - Foreground is set: net_rim_event_log_vi
a UI - NPWE RibbonLauncherApp@5259947e 5
a UI - NPWE RibbonLauncherApp@5259947e 6
a UI - NPWE RibbonLauncherApp@5259947e 7
W UniversalSearch - UniversalSearchUtilities : Unable to
a System - AMNF net_rim_bb_ribbon_app(93)
a AppManager - Foreground is set: net_rim_bb_ribbon_a
a AppManager - Foreground is requested: net_rim_bb_ri
```

BlackBerry Event Log Artifacts

Situation:

- Examiner has heard that **ALT+LGLG** will bring up event logs on a BB device.
- What sorts of relevant information are stored in Blackberry Event Logs?

Examiner Considerations:

- Bluetooth pairings
- When a slider model BlackBerry device has been manually slid open by the user
- Call history data that will be present even though it does not appear in the Phone Call Log or Phone History database areas.
- Event log data is volatile and can roll over in less than 24 hours, depending upon device activity.
- Run the UFED PA plugin for BlackBerry event log if you have a physical image of the BlackBerry device.
- Commercial tools that obtain the event log data:
    - Oxygen Forensic Suite (OFS)
    - UFED PA has a plugin for BlackBerry Event Logs
- A number of non-forensic tools can extract this data including BlackBerry Desktop Software.

7.0. BLACKBERRY MALWARE

BlackBerry Infected with Spyware or Malware

Situation:

- BlackBerry devices, assigned to company personnel, were used overseas on business travel.
- The BlackBerry devices that were turned on and accessed email, were prompted for a firmware update, which their respective device users completed.
- Upon return to their home network, a review of these firmware updated devices led to the discovery of oddly named files with very long filenames. Those files were not present in the BlackBerry devices that did not access email.

Examiner Considerations:

- As this is a firmware update, the device may have been compromised in a similar fashion to the Etisalat compromise.
- Isolate devices from network.
- Obtain physical and logical data acquisitions of device.
- Wipe devices and restore them to the latest home carrier issued firmware.
- Issue travel devices to users travelling to specific global regions.

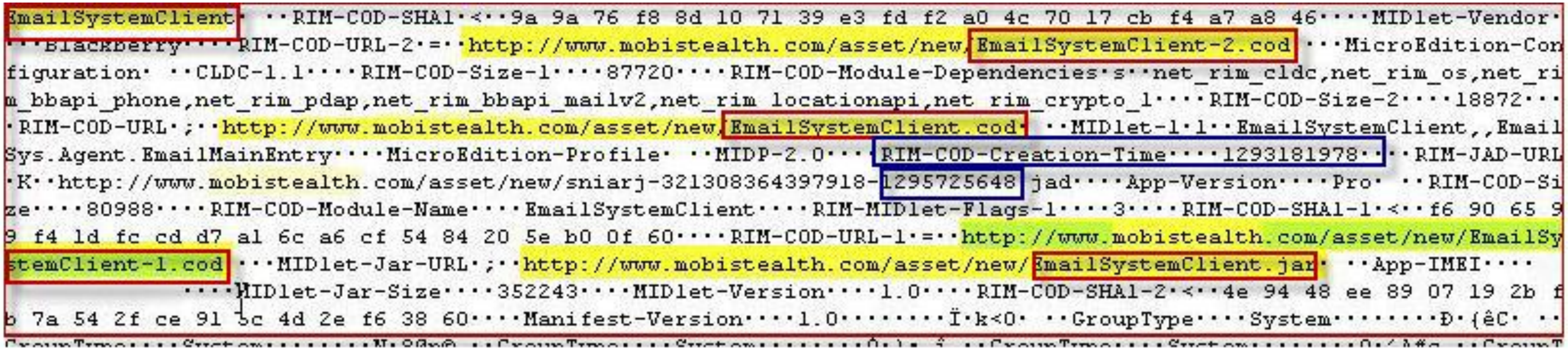
7.0. BLACKBERRY MALWARE

BlackBerry Infected with Spyware or Malware

Situation:

- Examiner has heard that BlackBerry is the safest Smartphone platform out there and is “immune” to malware.
- Victim claims phone is “bugged” and that s/he’s being stalked by an ex who knows their whereabouts, contents of texts, conversations, emails, and social networking communications
- Is victim mentally ill, or is their suspicion valid?

Examiner Considerations:



```
EmailSystemClient· ··RIM-COD-SHA1·<··9a 9a 76 f8 8d 10 71 39 e3 fd f2 a0 4c 70 17 cb f4 a7 a8 46····MIDlet-Vendor·
···BlackBerry····RIM-COD-URL-2·=··http://www.mobistealth.com/asset/new/EmailSystemClient-2.cod ···MicroEdition-Con
figuration· ··CLDC-1.1····RIM-COD-Size-1····87720····RIM-COD-Module-Dependencies·s··net_rim_cldc,net_rim_os,net_ri
m_bbapi_phone,net_rim_pdap,net_rim_bbapi_mailv2,net_rim locationapi,net rim_crypto_1····RIM-COD-Size-2····18872···
·RIM-COD-URL·;··http://www.mobistealth.com/asset/new/EmailSystemClient.cod· ··MIDlet-1·1··EmailSystemClient,,Email
Sys.Agent.EmailMainEntry···MicroEdition-Profile· ··MIDP-2.0···RIM-COD-Creation-Time···1293181978····RIM-JAD-URL
·K··http://www.mobistealth.com/asset/new/sniarj-321308364397918-1295725648 jad···App-Version···Pro· ··RIM-COD-Si
ze····80988····RIM-COD-Module-Name···EmailSystemClient····RIM-MIDlet-Flags-1····3····RIM-COD-SHA1-1·<··f6 90 65 9
9 f4 1d fc cd d7 a1 6c a6 cf 54 84 20 5e b0 0f 60····RIM-COD-URL-1·=··http://www.mobistealth.com/asset/new/EmailSy
stemClient-1.cod ···MIDlet-Jar-URL·;··http://www.mobistealth.com/asset/new/EmailSystemClient.jar· ··App-IMEI····
        ····MIDlet-Jar-Size···352243···MIDlet-Version····1.0····RIM-COD-SHA1-2·<··4e 94 48 ee 89 07 19 2b f
b 7a 54 2f ce 91 5c 4d 2e f6 38 60···Manifest-Version···1.0········Ï·k<0· ··GroupType···System·······Ð·{êC· ··
```

June-9-14

TEELtechnologies

8.0. BLACKBERRY 10

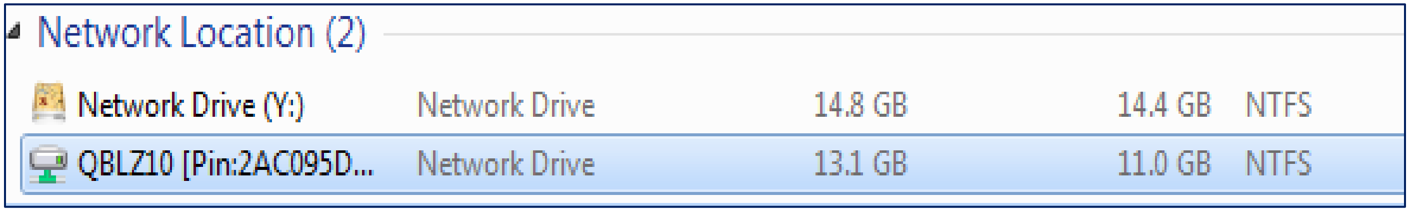
BlackBerry 10 Devices

Situation:

- Examiner received a Blackberry Playbook and a Z10 for examination.
- Now What?

Examiner Considerations:

- Limited forensic tool support for BB10.
  - Cellebrite UFED, Oxygen: Logical
- Chipoff extraction shows that data is still encrypted at chip level.
- Limited access to user data via “Storage and Access” settings using connection to Windows or Mac OS X computer.
  - Two NTFS partitions mounted upon connection



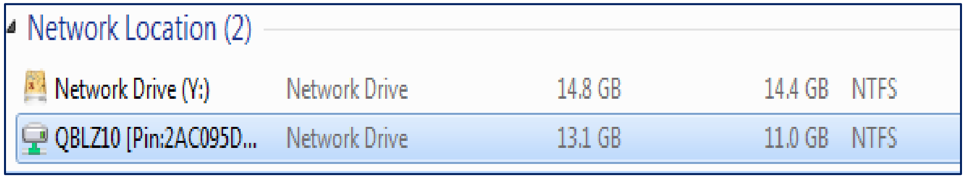
Network Location (2)

Network Drive (Y:)	Network Drive	14.8 GB	14.4 GB	NTFS
QBLZ10 [Pin:2AC095D...	Network Drive	13.1 GB	11.0 GB	NTFS

BLACKBERRY 10

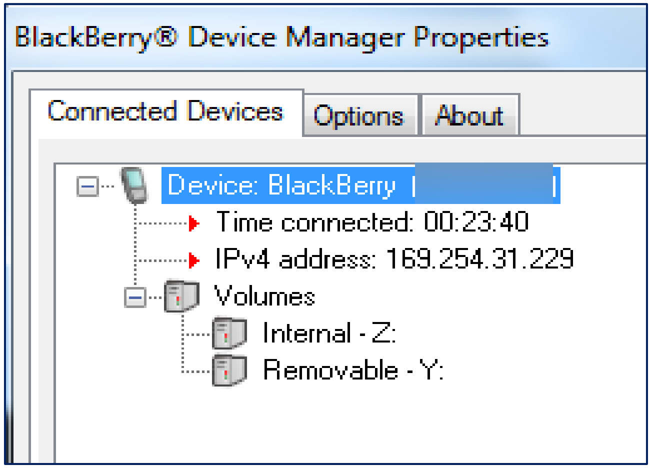
Connected to Windows 7 or Mac OS X:

- If the BB10 is password protected, password must be entered in BlackBerry Link, before volumes will mount.
  - Volume Z is internal memory
  - Volume Y is Removable SD card



Network Location (2)

Network Drive (Y:)	Network Drive	14.8 GB	14.4 GB	NTFS
QBLZ10 [Pin:2AC095D...	Network Drive	13.1 GB	11.0 GB	NTFS



BlackBerry® Device Manager Properties

Device: BlackBerry [redacted]

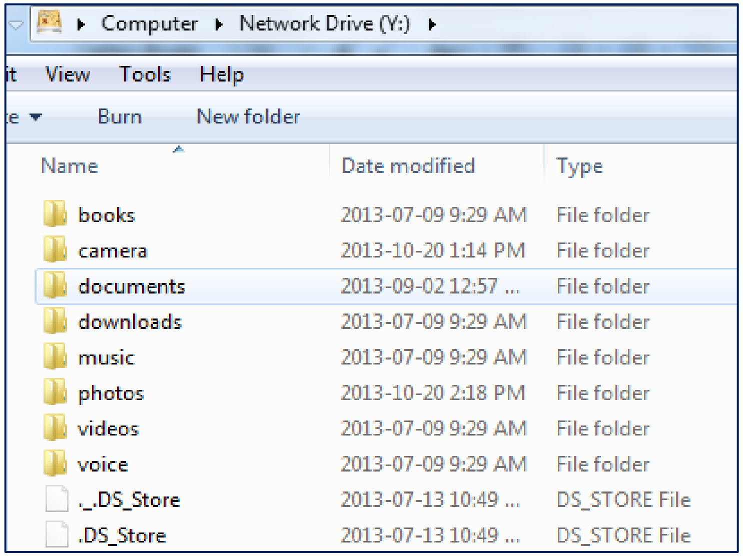
Time connected: 00:23:40

IPv4 address: 169.254.31.229

Volumes

Internal - Z:

Removable - Y:



Computer ▸ Network Drive (Y:) ▸

Name	Date modified	Type
books	2013-07-09 9:29 AM	File folder
camera	2013-10-20 1:14 PM	File folder
documents	2013-09-02 12:57 ...	File folder
downloads	2013-07-09 9:29 AM	File folder
music	2013-07-09 9:29 AM	File folder
photos	2013-10-20 2:18 PM	File folder
videos	2013-07-09 9:29 AM	File folder
voice	2013-07-09 9:29 AM	File folder
._.DS_Store	2013-07-13 10:49 ...	DS_STORE File
.DS_Store	2013-07-13 10:49 ...	DS_STORE File

June-9-14

8.0. BLACKBERRY 10

Unlocked BlackBerry Z10

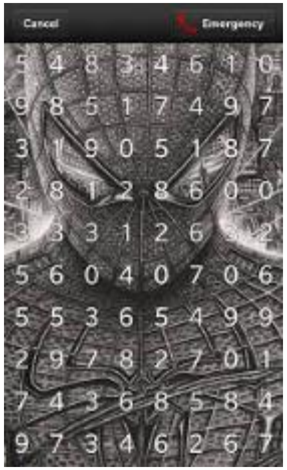
Situation:

- Unlocked BlackBerry Z10. Used BlackBerry Link Software to obtain a BBB backup.
- How can I read/parse this backup file? When I try and open the TAR archives within the BBB file, they look like they are encrypted.

Examiner Considerations:

- By default, the BBB backup of a BB10 device (and Playbook) made with BlackBerry Link is encrypted, even if the device has no password.
- There is no way to obtain an unencrypted backup.
- There is no known way to mount this BBB backup file in a virtual simulator.
- Oxygen Forensic Suite v6.1 and higher and latest version of Elcomsoft Phone Password Breaker can decrypt the BBB file provided you know the password to the BlackBerry ID account.
- Latest version of UFED hardware can perform a logical extraction of limited data from the BlackBerry 10 device.
- BlackBerry 10 backup contains:
  - SQLite databases in .db and .dat format
  - XML files
  - INI files
  - BIN files
  - And various other types of files with plain text content such as .conf files.

8.0. BLACKBERRY 10



Locked BlackBerry Z10

Situation:

- Locked BlackBerry Z10.
- Picture Password: if this is enabled, then a device password is also enabled as it is a pre-condition.
- Now dealing with two password mechanisms.

Examiner Considerations:

- No solution is available for any locked BlackBerry 10 device.
- Chipoff shows that data is still encrypted at chip level.

QUESTIONS?

- For more information, the full 206 page Power Point (in PDF) that this presentation was adapted from can be downloaded from OneDrive at: http://1drv.ms/1hKLmU1

- The presenters would be more than happy to sit down to discuss BlackBerry and Mobile Device Forensics related questions over a cold beer.

- Contact Information:
  - Shafik Punja: shafghp@gmail.com or qubytelogic@gmail.com
  - Cindy Murphy: CMurphy@cityofmadison.com